Date of publication July 31, 2022, date of current version Aug. 12, 2022.

A Conceptual Architecture for Monitoring Students in Zoom during Online Educational Sessions

PKSC Jayasinghe [1#], EHMPMWijerathna [1], and SY Rajapaksha[2]

[1]Department of Information and Communication Technology, Faculty of Technology, University of Ruhuna, Sri Lanka.
[2]School of IT and Computing, Sri Lanka Technological Campus, Ingiriya Road, Padukka. Sri Lanka.
[1#]subash@ictec.ruh.ac.lk

ABSTRACT Recently the education systems around the world have adhered to a distance learning/teaching method. However, this approach don't provide any guarantee that participated students are presented during the session. The given solution is suggested as an add-on feature in Zoom. This feature enables the teacher to detect the students' availability. The main objective of the architecture is to check the availability of students in the meeting time to time. In this architecture automatic image capturing and processing techniques are used. According to the proposed method images of students are captured automatically and periodically to a previously defined time i nterval. This is done by manipulating the camera in Android and making the preview of the camera invisible. The captured images are sent to the Zoom cloud to identify the identity of the student. Previously created image vectors (during training period) of students will be there to do the comparisons. Technologies like face embedding, Artificial Neural Network (ANN) are used in identification process of image p rocessing. If they are proven to be the legit participants, the students are accepted to the meeting from the waiting room. Periodically captured images are sent to the face detection by image processing using technologies as Viola Jones algorithm, Haar-like Features, AdaBoost algorithm, Cascading Classifiers, OpenCV. If the student is not available in the seat, a message is sent to the t eacher. Even though this conceptual architecture has few limitations, this will be a great help in detecting the students' identities and availability during learning/teaching environment.

INDEX TERMS: AI, Conceptual Architecture, Image Processing, Online sessions.

I INTRODUCTION

A *Background*

The world is evolving day by day and man with it. People are living in a technological era where technology is integrated into every field in human life. For health care, education, business field, and other day to day chores, technology has become an essential resource. The necessity of technology incorporation has become an inevitable change due to the current situation in the world. COVID -19 has changed the world's way into a new norm by reducing the human contact in the society. Especially the education systems all around the world have adhered to a distance learning/teaching method. As a result of that, education in all over the world has changed dramatically, with the distinctive rise of e-learning, whereby teaching and learning are undertaken remotely and on digital platforms.

In this situation online communication platforms as Zoom, MS Teams, Skype and Google Meet have become popular and has widely used by almost every country around the world. The mobile devices and laptops have become the new educational facilitator for most of the students and teachers in this new norm. Out of the wide range operating systems, Android is the most popular at present as exemplifies in Figure 1. When it comes to the global smartphone market, the Android operating system dominates the competition. According to Statista, in 2019 Android had an 87 percent share of the global market, while Apple's iOS had only 13 percent. This gap is expected to increase over the next few years [1]. Furthermore, Web analytics firm StatCounter reported that, for the first time ever, Android topped the worldwide OS internet usage market share. In March 2021, looking at combined usage across desktop, laptop, tablet and mobile, Android usage hit 37.93 percent. That was enough to narrowly overtake Windows' 37.91 percent [2]. Additionally, android provide the developers to experiment with its platform by providing the developer options. In a chaotic situation like this all these educational online platforms came as a blessing in disguise. These tools are used as the main lesson delivery method all around the world. These platforms have some social, technical and pedagogical drawbacks. According to the various researches done previously, there are some concerns that come with online learning. For instance, there are several

issues on the internet bandwidth, internet connection, lack of human interaction, disturbances coming from home environment, students not communicating during the virtual classes, teachers' not being able to track the students improvement or engagement in class and not being able to cope up with the technologies are some of them [3], [4], [5].

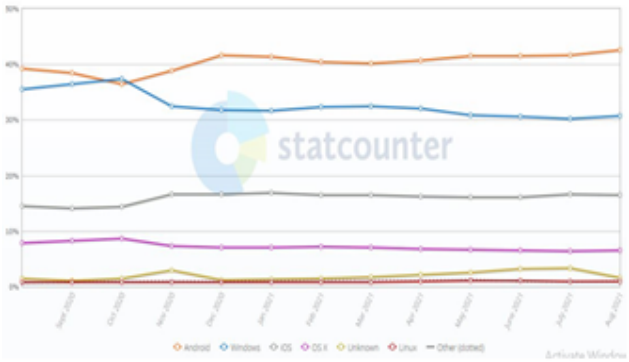

Figure 1. Desktop, Mobile and Tablet OS market share worldwide
Source: Global Statistics (Aug 2020- Aug 2021)

Out of those issues, this research focuses on one technical drawback that teachers/lecturers are facing due to the digitalization of physical classes. As many students had often choose to leave their cameras off [6], it is hard for the lecturers/teachers to find whether the students are presented on the other side or not. However not pressurizing students to turn on their camera is considered as the best student-centered policy during online classroom according to the research done by Costa because some students do not have access to a private space or are embarrassed of their home environment and sometimes they don't have the necessary technical equipment, resources and not being economically feasible to afford flawless internet connection [7]. Therefore considering these both sides (teachers and students), the main objective of this study is to find a technological solution for this issue by making Zoom platform to detect whether the students are actively participating for the session or not by using a combination of several methodologies without making students to turn on their cameras. The Android platform is considered in developing this architecture because as mentioned prior, Android is the widely used platform around the world and the developer freedom in Android is higher than any other platforms.

B Literature Review

In the digital world anything is possible if people know how to manipulate their electronic surrounding properly. Human curiosity and experiments have paved the way for the implement various useful features and apps in technology. In the field of cyber security, the spy wares that are used to spy on people by controlling the device camera is one example for the misuse of knowledge. In 2013 Edward Snowden revealed NSA (National Security Agency) have the ability to watch and spy on users by their laptop/desktop or phone camera at any time, without even having approval or knowledge of the user. Likewise there have being many incidents where hackers has used these spywares to automatically capture live images and videos of people. This newly found knowledge of accessing the cameras of digital devices has coined a new attack term called "Camfecting" in modern technological world [8]. Recently this feature of manipulating the camera to automatically capture images are being used in several researches in different scenarios. Dong et al. developed automatic image capturing and processing for PetrolWatch [9]. This method use to capture a clear image by an unassisted mobile phone from a moving car by manipulating the camera control of the mobile phone and by using image pre-selection schemes. Furthermore, in the study done by Aldaz et al. exemplifies how to automatically capture image through leveraging the sensor capabilities of Google Glass, where SnapCap enables hands-free digital image capture, and the tagging and transfer of images to a patient's EMR [10].

Bah and Ming proposed a methodology to improve face recognition algorithm for attendance management system as the practical application of the suggested algorithm [11]. The existing computer applications of face recognition is able to detect, identify and verify human faces from an image or video for security, identification and attendance purposes. But still some issues are identified which are affected to the accuracy of the face recognition process. Some identified issues are variations and differences in human face due to different lighting conditions, noises in images, different poses/appearances of the face and scale/resolution changes of the image etc. As a solution for that they suggested a new methodology to increase the overall accuracy of the face recognition system. This proposed method was implemented by using Local Binary Pattern (LBP) algorithm with some advanced image processing techniques such as contrast adjustment, bilateral filter, histogram equalization and image blending. However, this finding is unable to address the issue of occlusion and mask faces in face detection and recognition.

Singh and Goel suggested an improvement for the methods of detecting and recognizing human faces by using digital image processing [12]. The suggested improvements consisted with two phases such as detecting a face and identifying the face as an individual from images. In the first phase, face detection process avoided the objects which are placed quite far as a limitation of that approach. The second phase authenticated the identity of the human face by using unique facial characteristics. The above suggested technique is based on biometric technology combined with digital images processing techniques such

as the Eigenface method, Fisherface method and PCA (Principal Component Analysis).

Pandey et al. reported a new method to develop a real time parallel vision system based on human face identification for Home Service Robot (HSR) by using real-time image processing techniques [13]. It is a computer application to identify and verify a person automatically from digital image or a video frame from a video source. This suggested system consisted with different sub-systems based on adaptive skin detector, condensation filter with parallel computing particles, Haar-like classifier and a simple and fast motion predictor for tracking, detecting and identifying a human face. The developed system is only able to detect and recognize limited number of human faces. As a solution for that limitation, the study suggested to create much wider database with larger space for recognizing any number of human faces.

II METHODOLOGY AND EXPERIMENTAL DESIGN

A Suggested System Model

The user (student) identification and detection methodologies are incremental approaches which are used to detect the face of the student and recognize the identity of the student from the captured images by using image capturing process. The inputs for these user identification and detection processes are captured images and the detected result as whether the student is really seated or not for the lecture/session is sent to the lecturer/teacher who is a host for the Zoom meeting as the final output. Basically, this methodology consists with four main sections namely image capturing, model training, user identification and user detection. Figure 2 illustrates the overview of this suggested system model.

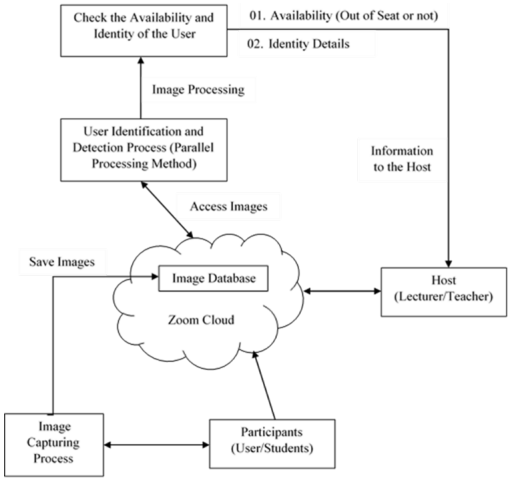

Figure 2. Overview of the suggested system model.

Above suggested solution can be added as an add-on to the Zoom tool where it will provide a feature to turn on according to the user's (lecturer/teacher) requirement.

B Training Process

As the initial step of this proposed methodology, training/classifier model should be created. The multiple images of students' faces are used as the training dataset for this classifier model. As the method of taking images of the individual student, in the initial Zoom meeting minimum 50 images of the student should be captured automatically by using image capturing process which is discussed in the section 2.3 in this paper, with every two minutes time gap.

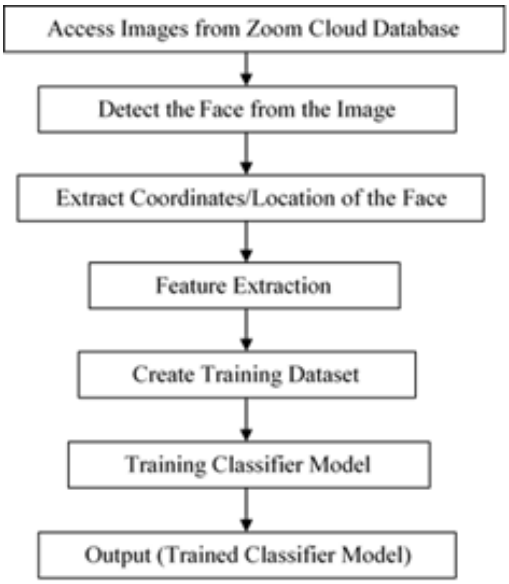

Figure 3. Overview of the training process.

There should be minimum 50 images per student to increase the accuracy of the training model and increasing the number of images per student (increasing the training dataset) can be able to get the highest accuracy from the training model. The above captured images of the students are stored in the Zoom cloud database as separate folders for individuals for the training model. These images are accessed as the input training image dataset for the classifier model. Figure 3 illustrates the main steps of this training process.

As the first step of the training process, student's face should be detected from the image. This suggested face detection methodology is discussed in section E in this paper. Then the exact locations/coordinates of the detected face are identified and the face is extracted/cropped by using these identified locations/coordinates. The features are extracted out of the cropped face as the feature extraction process and a pre-trained neural network is used to extract these features. An image of the student's cropped face is taken as an input for this neural network and it

outputs a vector which represents the most important features of a face. According to the machine learning, this feature vector is called as face embedding [14]. The dlib and the face_recognition libraries in OpenCV are pre-trained neural network libraries and these libraries contain implementation of deep learning which are used to construct face embeddings (feature vectors) for training and the actual identification process [14].

An Artificial Neural Network (ANN) is used to train this suggested classifier model. An input dataset of this ANN classifier model is created by using above extracted face embeddings (feature vectors). The keras and tensorflow libraries and sequential keras model with dense type keras layers are used for creating this Artificial Neural Network [15]. There is an input layer, hidden layers with several neurons per each hidden layer and output layer. The number of hidden layers and the number of neurons per each hidden layer can be vary according to the input dataset. The output layer consists with several nodes for the expected output values and any specific or auto-generated indexes can be assigned as these expected output values for the students. After successful training of this classifier model, it is stored in Zoom cloud to use in the identification process of the participant (student).

C *Image Capturing Process*

The first step of the procedure is to capture the photo automatically of the person and then to send it to the image processing to clarify the identity and availability of the person in front of the camera. Therefore the camera should be able to capture a photo of the student automatically according to a given timeline. The best method would be not changing the current functions of the inbuilt camera of the system because it can cause security issues. The study suggests to include a camera as an element of Zoom app. This camera can be given a user-preferred install option while installing Zoom because this is only needed by students rather than the other users of Zoom. The overall process of the image capturing is illustrated by using Figure 4. (In here, an assumption should be made as the Zoom camera is installed during the installation of the Zoom app). The steps given in Figure 4 are further explained as follows.

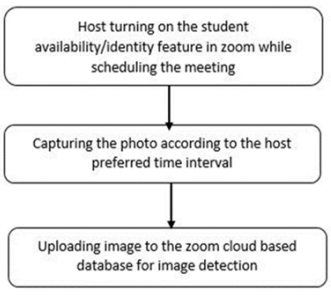

Figure 4. Overview of the image capturing process

1 *Giving the permission/turning on the feature to detect students in the other side:*

The host or the admin should turn on this feature in Zoom platform when creating the link. This is given as an add-on only in the Zoom platform. When the admin turn on this feature it will be activated to that particular meeting.

2 *Capturing a photo according to the given time intervals:*

After giving the permission to the process, capturing the image is the initial and the key part of this solution. This is done using the installed Zoom camera of the mobile or the laptop. It is assumed that the permission to access the camera is already given to the Zoom app when installing. The camera of the device (laptop or mobile) captures the photo of the student without their knowledge. The device will not show any preview of the camera to the student. The techniques and technological methods used in spywares to take photos in a legal form. These photos are later sent to the Zoom cloud where the image processing occurs.

Students can use different types of platforms to join a Zoom lecture or a lesson. Some can use laptop while others use mobiles or tabs like devices. Therefore the Operating System (OS) should be compatible with the proposed solution. Given below are the analysis of capturing the photo according to the three different OS platforms. The considered platforms are Windows, IOS and Android.

In Android it is possible to capture a photo without a preview and without disturbing the student. There are various developer options to control the camera in Android. There are numerous apps that has put this mechanism into practice where they are capturing a photo without a preview (for example: “quick camera” app, “Mobile hidden camera” apps). That same method of manipulating the camera can be done in a legal manner with Android since this is given as an embedded feature in Zoom. However in this method, because it is developed as a legally accepted feature, the student should have given camera access permission to Zoom when installing the Zoom app’s camera.

Therefore out of these three platforms, Android platform is considered in developing this solution as Android devices are used often by students and it is possible to build the solution with the help of Android developer option. Android provides full access to the device camera hardware. The camera control methods are one of these developer privileges that it provides for the developers. In this scenario, when capturing the image of the student, the preview of the camsera should be invisible or should be hard to glimpse. In Android this can be done by manipulating the camera object and the preview class. The

setVisibility() function in startPreview() function, can be set as this.setVisibility(INVISIBLE) to make the surface invisible as soon as it is created or the preview size can be set to 1x1 px, which will make the preview hard to detect. By following these types of camera control methods given by Android in the camera class, the image can be captured without alarming the student on the other side.

Another important feature of this part is the time intervals that photos are captures. The time intervals are configured as random times schedules (the minimum gap between the photo capture is five minutes) and the host is able to choose his/her preferred time interval. The reason for going for a random time intervals is due to the limitation that it has in windows camera access. In windows when accessing the camera the LED is turned on. If it is configured for fixed intervals the student will be able to understand the pattern. Therefore in order to reduce the impact of that limitation the random intervals for image capturing is decided. The minimum gap between two image captures is set to five minutes to give enough time to upload the photo into cloud and to conduct the image processing. Setting a timer to the camera in Android can be implemented by the handler class in java. Image resolution is a crucial factor when it comes to the image processing. The resolution of the photo should be a constant, however the resolution can be changed because of the different qualities of the inbuilt cameras of the devices. Therefore after the photo is captured it is converted in to a common resolution which is the minimum quality that is needed for image processing.

3 Sending it to image processing to clarify the identity:

After capturing the image according to the given intervals, that image is sent/uploaded to the Zoom cloud where the image processing taking place. Along with the captured image of the participant the device identification is sent. The device identification (device name/email name that the profile is created/ profile name, MAC address) is captured and sent along with that particular participant's image. This is done in each and every Zoom meeting sessions. By sending the device identification, it will help the system to understand whom should be accepted and whom should be rejected after the participant identification results arrived. When uploading the image for the image processing, the crucial feature would be the image quality and size. In order for image processing mechanism to work effectively the photo will be set to a common size and a common quality.

D User Identification Process

User identification is the process of recognizing the identity of the participant (student) as actually the real student or any other person participates the lecture/session. This process is more important in commercial education like tuition because lecturer/teacher is able to identify the actual identity of the students to give permission only to the authorized students.

While the students are joining the session through Zoom tool, the images are automatically captured. This image capturing process is further explained in section C in this paper. These captured images with respective device identity details of the students are sent to perform the suggested identification process. The above mentioned device identity details are valid only for the particular Zoom session and these details should be sent along with the captured image in every login to the session. Then by using this suggested identification approach, the students are identified and their identity details are sent with the respective device identity details to the Zoom for the acceptance of their login to the session. If there is a mismatch of the detected identity with the real identity of the students, then they are kept in the waiting room without giving access to join the session. If the student's identification details are correct, then they would be able to join the session as a legit participant. This suggested identification methodology should be processed as parallel processing because the images of all the students of the class should be processed at same time for identification purpose [16]. Figure 5 illustrates the main steps of this proposed identification approach.

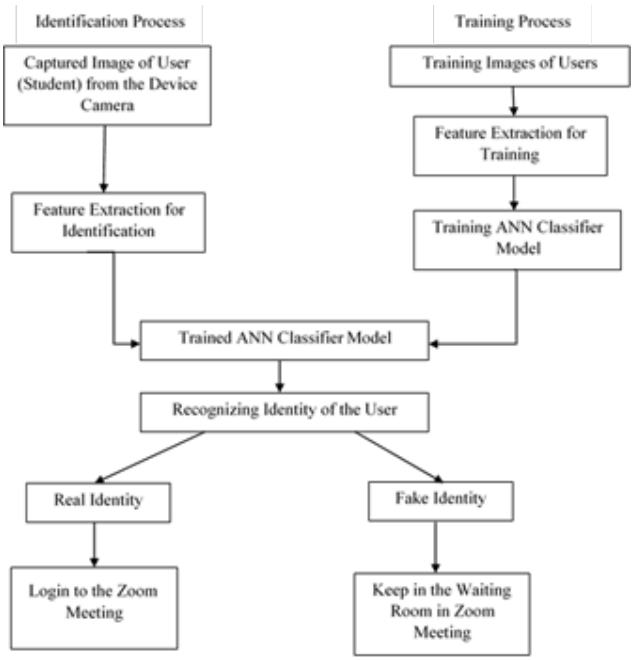

Figure 5. Overview of the User Identification Process.

As the first step of this identification process, when student is joined the zoom meeting, an image is captured automatically and student's face is detected by using that captured image. The suggested face detection methodology is discussed descriptively in section E in this paper. Finally, with the use of detected face of the student, it is successfully recognize whether the student's identity is real or fake which is the final outcome of this approach.

E User Detection Process

User detection is the process to clarify about the presence or the absence of the participant (student) for a long time period from the lecture/session. For this proposed detection methodology, the images of the students are randomly captured during the Zoom meeting. This image capturing process is discussed in section C in this paper. This suggested detection approach should be processed as parallel processing method because these captured images of all students in the class should be processed as parallel to detect the availability of the students during the Zoom meeting [16].

The captured images of the student are pre-processed as the first step and these pre-processed images are used to extract features and all of these extracted features are not useful and important. Therefore extracted features should be optimized for the classification process. If there is a face on the images, it can be detected as the output from this process. If the face is not detected as the outcome, then a message is sent with the identity details of the student to the host (lecturer/teacher) in the zoom meeting to notify about the absence of the relevant student. This suggested user detection process is used the Viola Jones algorithm, AdaBoost algorithm and cascading classifiers to determine whether there is any face in an image or not [17]. This process can be further subdivided as extracting features of the face, optimizing extracted features and classification process. Figure 6 illustrates the main steps of this approach.

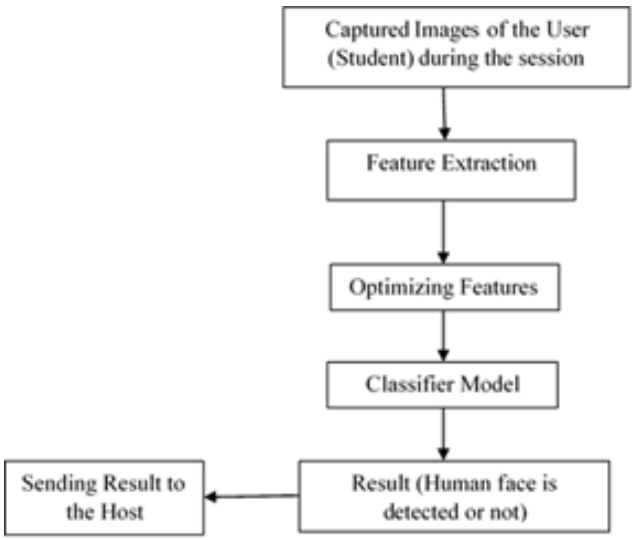

Figure 6. Overview of the User Detection Process.

1 Extracting features of the face:

Before go through the feature extraction process, image should be converted to a grayscale format by using cvtColor() function in OpenCV as the image pre-processing [18] because it can simplify the complexity of the image and it leads the way to achieve more effective results. In addition to that it can increase the speed of the image processing.

After image pre-processing, the Viola Jones algorithm is used to continue the feature extraction process. This algorithm is used Haar-like features which are called as digital image features to detect a face by looking at many smaller sub regions of the image for some specific features. All human faces have some universal properties like eyes region, nose region etc. The lightness and the darkness of pixels in the regions are used to recognize these unique properties in the human face. The sum of the pixel values is used to identify the regions as summation value of darker region is smaller than the summation value of lighter region. When it is dealing with large features, these computations can be very complex and it needs to be performed for each feature. As a solution for this problem, integral images are used to perform these computations quickly. Then by using this process, features of the image can be extracted for the optimizing process [17].

2 Optimizing extracted features:

There are different sizes of detector windows which are used to find and match the face in the image by using above extracted features. The one popular detector window is 24x24 detector window which has nearly 160000 number of features available. But there are only a few of these features which are important to identify a face. The AdaBoost algorithm which is a machine learning algorithm for identifying the best features among the huge number of features, is used to optimize these 160000 number of features in to around the best and the important 2500 features for detecting a face [17].

3 Classification process:

The above mentioned 24x24 detector window is used to slide over the image to detect whether any region contains a face or not. Also the cascading classifiers are used to discard non-faces, and avoid wasting time and computations. This cascading classifiers are used to divide the process of detecting a face into multiple stages. The best features such as eye region, nose region etc. are used for the first stage classifier and all the other remaining features are used for the next stages as second stage classifier, third stage classifier etc. When an image sub region enters the cascading classifiers, the first stage is evaluated for identifying its features and if it gets result as positive, meaning that it thinks it can be a face and the output of the stage is, “it may be a face”. When a sub region gets that result, it is sent to the next stage of the classifiers and the process continues until it reach the last stage. If all the classifiers give positive output, then it is classified as a human face and if any stage from beginning to last gives

negative output then image is immediately discarded since it is detected not as a human face [17].

OpenCV comes with a lot of pre-trained Haar cascade classifiers such as classifiers for smile, eyes, face, etc. For making this detection process simple and easy, these pre-trained Haar cascade classifiers also can be used along with the CascadeClassifier() function. detectMultiscale module of the classifier can be used to detect the face and it can return coordinates of the detected face as output [18]. Finally it is able to detect the student's face from the image with the coordinates as the result from this approach.

III RESULTS AND DISCUSSION

The main objective of this proposed architecture is to detect the presence or the absence and the real identity of the participant (student) on other side. As the result of the image capturing process, the images of the students are successfully captured without disturbing them. As the output of the detection approach, the host (teacher/lecturer) is able to detect whether the students are participating for the session or not without making them to turn on their device camera. It is more flexible way for both sides (teachers and students) and it can improve the efficiency and activeness of both online teaching and learning. As the outcome of the identification approach, the real identity of the student is successfully detected. Moreover, this approach is very useful and effective in commercial education like tuition because lecturer/teacher is able to give permission only to the authorized students.

Given below are two test cases for a valid user (participant A) and an invalid user (participant B) respectively to further explain the above summary of the results.

A Test case for participant A (valid) and B (invalid)

1 Identification Process for Participant A (Figure 7) and B (Figure 9):

The participant A, who is a legit/valid participant for the particular online educational session, is logged to the Zoom meeting. The participant B who is not a legit participant for the particular class is also logged into the Zoom session. After logging in, all the participants are kept in the waiting room for the identification process. While participant A and B are in the waiting room, images of both participants are automatically captured. This captured images of the participant A and B are then sent to the Zoom cloud database with the device identification details of each, to perform the identification process. During this process, trained classifier model compares the features of the captured image of the participant A and give the result as the detected identity is matched with the real identity. Then the participant A is considered as a legit/valid participant for the session. The device identification details of the participant A along with his identity details are sent to the Zoom for the acceptance of the login. As the final step of this approach, the participant A is able to join the session as a legit/valid participant.

While for the participant B, the comparison done by the classifier model decides that participant B is not a legit participant for this class. That result is then sent to the Zoom along with the device identification of the participant B. Since it will be given as an unauthorized participant, the participant B is not admitted to the Zoom session. Hence, he is kept in the waiting room.

2 Detection Process for Participant A (Figure 8):

After performing the identification process, the participant A is accepted to the online session as an authorized participant. The images of the participant A are randomly taken during the Zoom meeting. The above captured images are sent to the Zoom cloud database for the detecting process to verify the presence or the absence of the participant A in time to time. In detection approach, the above captured image is processed to detect the human face on it as the final outcome. If the participant A is not in the seat, it is recognized by the detection process and notify the host (teacher/lecturer) by sending a message with his identity details. Then the host is able to detect the absence of the participant A.

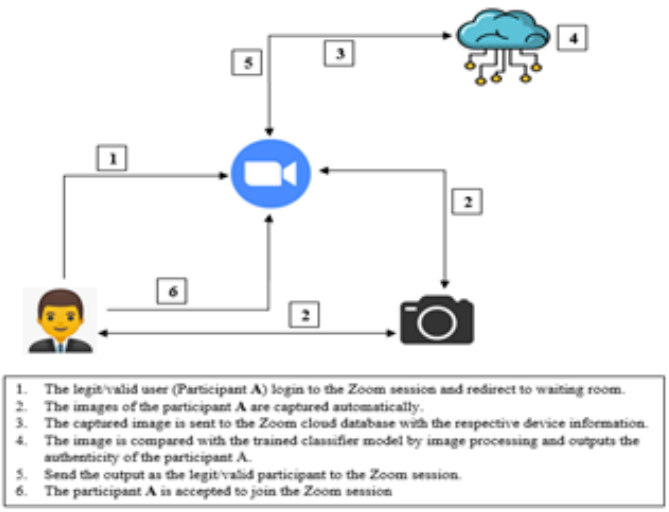

Figure 7. Valid participant A – Identification process

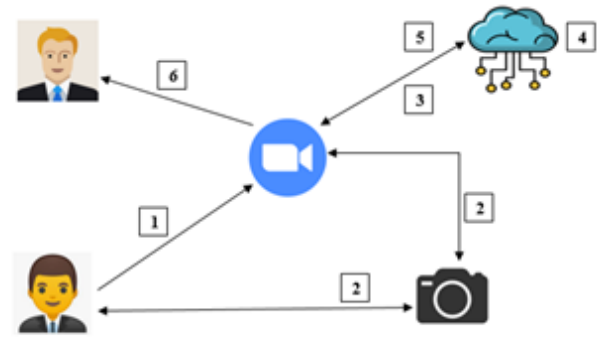

Figure 8. Valid participant A – Detection process.

Figure 9. Invalid participant B – Identification process.

Even though in this framework is considering only Android OS, the covert image capturing can be implemented for Windows and IOS as well. For example in windows the camera of the laptop can be accessed through manipulating firmware/BIOS of the system. However, since this is proposed as an inbuilt feature for Zoom, accessing the camera illegally won't be necessary. The only issue in accessing the camera in Windows platform is the LED bulb that is embedded in the laptop. The light also can be turned off as some spyware software does, however if the camera light is connected by a hardware mechanism it is hard to turn off the light while capturing the photo. In that case the random photo capturing intervals will be a blessing in disguise, because even though it is complex than static time intervals, it will stop from making students to find out about the pattern of photo capturing.

Implementing this architecture in Mac OS is slightly challenging than the other two operating systems. However it is not impossible as there are apps that are used to take covert images of others using IPhone's inbuilt camera like "SneakyPix" app. Nevertheless, for this operating system also the student should have given the camera access permission to Zoom as it is coming as a default feature in Zoom.

IV CONCLUSION

This study propose a conceptual architecture to monitor whether the students are participating for the session or not and the real identity of students without forcing them to turn on their camera. It is suggested as an add-on to the Zoom tool where it will provide a feature to turn on according to the user's (teacher) requirement. Since the user detection and identification processes occur concurrently during session the processing time can be high. Therefore, as a solution for that issue, parallel processing techniques are suggested. According to the study, it is only discussed on Android OS platform but there is a scope to carry out further research on implementing it in other different OS platforms like Windows and Mac can be implemented as further works.

Nowadays the online communication platforms such as Zoom, MS Teams, Skype and Google Meet have become popular and are widely used by almost every country around the world. The proposed architecture provide solution only for Zoom platform. However, other different online communication platforms can also be implemented according to this proposed architecture.

This proposed architecture will assure the fact that students will not boycott the educational sessions even though it is in a virtual platform. It will make the online education to go one step forward in adopting the effectiveness of a physical classroom. The students' availability will be monitored even their cameras' are turned off which will give the upper hand to the host of the educational session. It will allow students to learn efficiently as they are learning in a physical classroom.

Additionally, this solution will be an advantageous movement for online exam proctoring and for private tuition classes because of the proposed identification process of the participants. The invigilator or the teacher will be able to identify the authenticity of the logged in student with this Zoom add on. With the current situation in the world, the online/virtual education will be the only solution to conduct the lessons. Therefore it is an utmost necessity to identify the issues in virtual education and to propose solutions for them to make it more effective.

REFERENCES

[1] J. Cohen, IOS More Popular in Japan and US, Android Dominates in China and India, Available: https://www.pcmag.com/news/ios-more-popular-in-japan-and-us-android-dominates-in-china-and-india, 2020, Accessed: 03 August 2021.

[2] M. Smith, Privacy and security fanatic, CSO, Available: https://www.csoonline.com/article/3187011/android-is-now-the-worlds-most-popular-operating-system.html, 2017, Accessed: 03 August 2021.

[3] V. Saminathan, Problems of online classes, International Journal of Academic Research Reflector, vol. 9, pp. 1-3, 2020, DOI: 10.6084/m9.figshare.13573550.

[4] A. Ullah, M. Ashraf, S. Ashraf and S. Ahmed, Challenges of online learning during the COVID-19 pandemic encountered by students in Pakistan, Journal of Pedagogical Sociology and Psychology vol. 3(1), pp. 36-44, 2021, DOI: http://www.doi.org/10.33902/JPSP.2021167264.

[5] M. Mahyoob, Challenges of e-Learning during the COVID-19 Pandemic Experienced by EFL Learners, Arab World English Journal (AWEJ), vol. 11(4), pp. 351-362, 2020, DOI: https://dx.doi.org/10.24093/awej/vol11no4.23.

[6] F. R. Castelli, M. A. Sarvary, Why students do not turn on their video cameras during online classes and an equitable and inclusive plan to encourage them to do so, Academic practice in ecology and evolution, vol. 11(8), pp. 3565-3576, 2021, DOI: https://doi.org/10.1002/ece3.7123.

[7] K. Costa, Cameras be damned, Available: https://www.linkedin.com/pulse/cameras-damned-karen-costa/, 2020, Accessed: 04 August 2021

[8] A. Sommacal, Camfecting: what it is and how we can protect ourselves from it, UNIlab blog, Available: https://www.unilab.eu/articles/coffee-break/camfecting/, 2018, Accessed: 07 August 2021.

[9] Y. Dong, S. Kanhere, C. T. Chou, and R. Liu, Automatic image capturing and processing for PetrolWatch, Proceedings of the ICON 2011 - 17th IEEE International Conference on Networks, pp. 236-240, 2011, DOI: 10.1109/ICON.2011.6168481.

[10] G. Aldaz, L.A. Shluzas, D. Pickham, O. Eris, J. Sadler, S. Joshi and L. Leifer, Hands-free image capture, data tagging and transfer using google glass: a pilot study for improved wound care management, Plos One vol. 10(4), 2015, DOI: https://doi.org/10.1371/journal.pone.0121179.

[11] S.M. Bah, F. Ming, An improved face recognition algorithm and its application in attendance management system, Array, vol. 5 (100014), 2020, DOI: https://doi.org/10.1016/j.array.2019.100014.

[12] G. Singh, A.K. Goel, Face Detection and Recognition System using Digital Image Processing, 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 348-352, 2020, DOI: 10.1109/ICIMIA48430.2020.9074838.

[13] K. Pandey, R. Lilani, P. Naik, G. Pol, Human Face Recognition Using Image Processing, International Journal of Engineering Research and Technology (IJERT) vol. 2(04), 2014.

[14] H. Mujtaba, Face Recognition with Python and OpenCV, Available: https://www.mygreatlearning.com/blog/face-recognition/, 2021, Accessed: 05 August 2021.

[15] P. Wijerathna, L. Ranathunga, Rice Category Identification using Heuristic Feature Guided Machine Vision Approach, IEEE 13th International Conference on Industrial and Information Systems (ICIIS 2018), pp. 185-190, 2018, DOI: https://doi.org/10.1109/ICIINFS.2018.8721396.

[16] S. Yalamanchili, J.K. Aggarwal, Parallel Processing Methodologies for Image Processing and Computer Vision, Advances in Electronics and Electron Physics, vol. 87, pp. 259-300, 1993, DOI: https://doi.org/10.1016/S0065-2539(08)60018-9 .

[17] H. Mujtaba, Face Detection using Viola Jones Algorithm, Available: https://www.mygreatlearning.com/blog/viola-jones-algorithm/?highlight=face

[18] P. Pandey, Face Detection with Python using OpenCV, Available: https://www.datacamp.com/community/tutorials/face-detection-python-opencv, 2018, Accessed: 02 August 2021.

AUTHOR BIOGRAPHIES

Dr. P.K.S.C. Jayasinghe attached to the Department of ICT, Faculty of Technology, University of Ruhuna. Presently he serve as the head of the department. He has number of research pub-lications in both journals and symposiums related to IT domain.

E.H.M.P.M.Wijerathna attached to the department of ICT, Faculty of Technology, University of Ruhuna as the lecturer. Her main research interest is image processing. She has several research publications on this field.

S. Y. Rajapaksha works as the lec-ture in School of IT and Computing, Sri Lanka Technological Campus. She worked in Department of ICT, Faculty of Technology, University of Ruhuna as a temporary lecturer. She graduated in SLIIT specializing in Cyber security. She has several publications related to the Cyber security.